YOUR GADGETS ARE SPYING ON YOU

Hackers can observe you through your PC's webcam, TV device or mobile phone. We show you what such hackers can do and how to protect yourselves.

BY **CHRISTOPH SCHMIDT**

Your television can watch you while you're watching it; your notebook can follow you when you surf the Web and your smartphone can secretly scan every corner of your house. All these pictures could then land in the hands of hackers. Such a scenario may sound like part of a Michael Bay movie, but it is a real threat, as our connected devices are equipped with cameras that are not well protected and can allow people unauthorised access with relative ease.

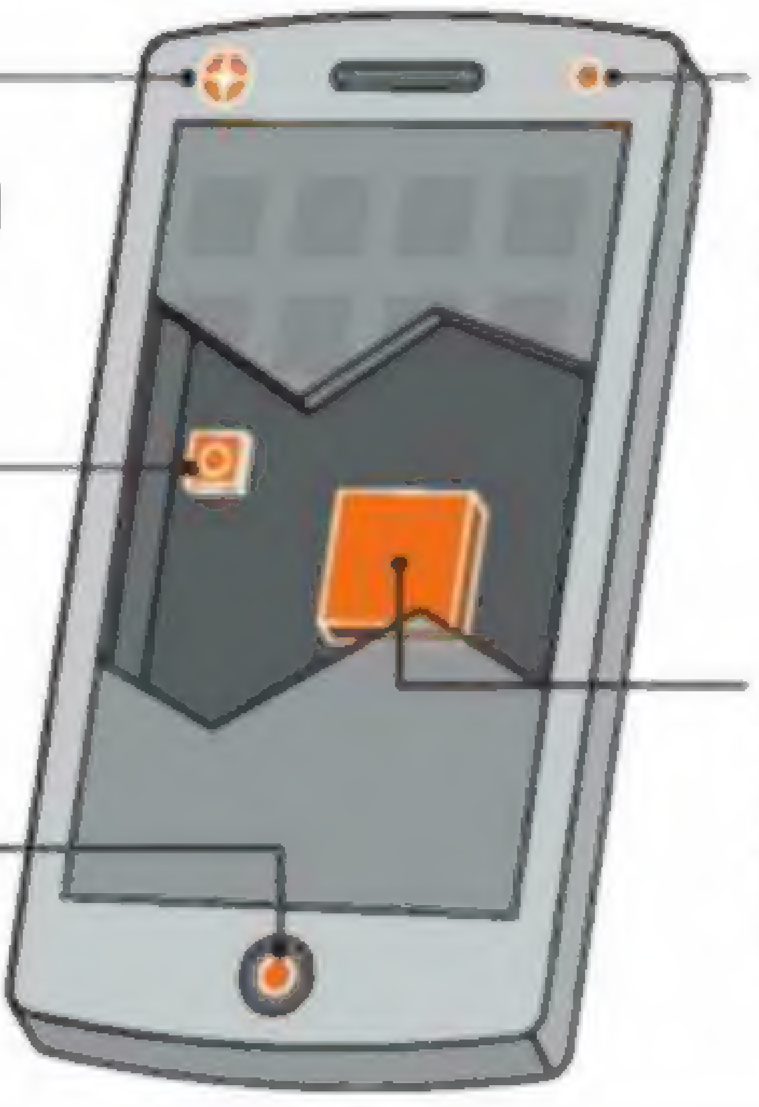
There have been cases of PC rental agencies exploiting such weaknesses to track their customers and even schools have tracked students without their knowledge. Amongst the many things these spying mechanisms allow hackers to do is install malware. And some of the more malicious PC malwares can even lock up a PC and threaten to delete everything on it unless you pay a ransom, and an image of yourself through your own webcam is shown to show you proof of your being monitored.

High-quality detailed image of your apartment

The consequences can be much more drastic if a malicious hacker takes over your mobile phone cameras. Since they are used at many locations and are always moving, phones can be used to extrapolate detailed, variable, zoomable panorama shots of apartments and offices. Papers strewn across an office and notices on boards can be read. Scientists have already developed proof-of-concept software to create high-resolution images from such cameras. Besides PCs and smartphones, there are also smart TVs with integrated webcams that can be misused. We show you how dangerous the situation is and how to protect yourself from your own devices.

SMARTPHONES: THE MOST PRIZED TARGET FOR HACKERS

The smartphone is especially rewarding due to the large number of potentially hackable sensors. By secretly taking photos, an attacker can read the embedded GPS information and discover your exact location.



COMPASS / GPS: Accurate location information can be used for planning a robbery

SENSORS: The accelerometer can detect keystrokes on a PC keyboard

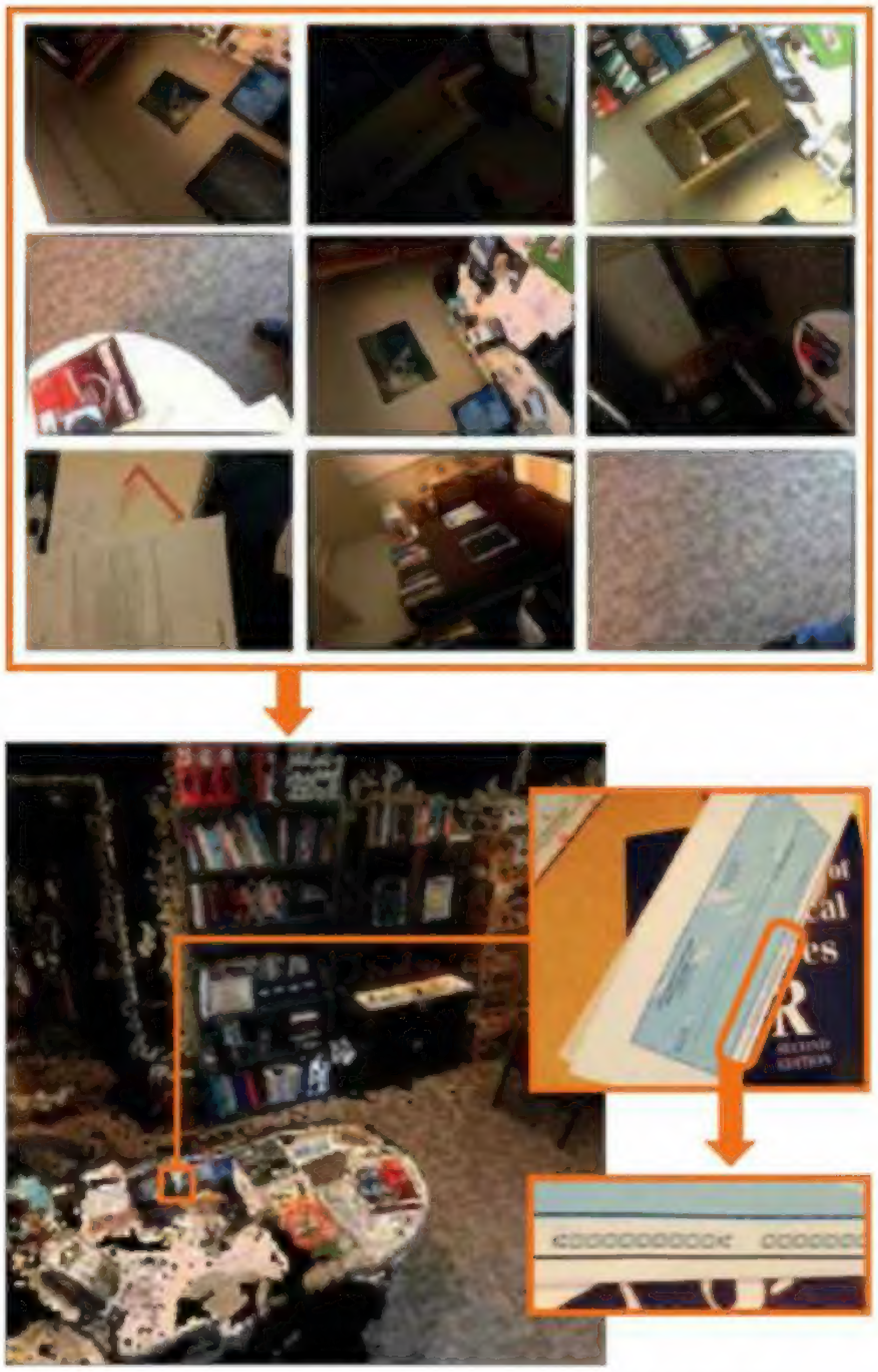
MICROPHONE: Calls may be monitored and voices recorded

WEBCAM: The smartphone provides hundreds of photos that can be combined into a large 3D model

3G: Your smartphone can be triangulated and its position located using cellular antenna towers

A TROJAN THAT SCANS YOUR ENTIRE APARTMENT

Researchers have developed a smartphone Trojan called Place Raider, which regularly takes photos and uploads them to a server without a user's knowledge. A virtual walkthrough of any location can be reconstructed from the multiple images.



Post-processing algorithms can use multiple photos to extrapolate a very sharp close-up of an object.

SMARTPHONE

The Eye of Sauron

A smartphone can reveal intimate details about you not only through its camera but with its other sensors too.

With an active Internet connection, one or even two cameras and other sensors, your smartphone is an especially rewarding target for hackers on a mission. Unlike a stationary PC, it not only includes potentially compromising photos but a range of information that can be called up together with images connecting you to it—including details such as where and when the photo was taken. Researchers have already manipulated smartphones to create extensive and zoomable panoramas of a room by combining and interpolating a number of secretly taken photos. They could then simply flick through the composite image to find important information.

Even manufacturers of smartphones and their business partners are desperately interested in collecting such information. One such example is ad tracking, which Apple has introduced with iOS 6. It works by assigning a unique number that associates a user with a particular device. When visiting websites and whilst using apps, this number is sent to advertising servers whose operators get an exact picture of what interests you, and which advertisements you'd be more likely to act upon.

Espionage through mobile phone microphones and sensors

If you think your smartphone and its webcam are protected by Android's security mechanisms, think again. The operating system is dependent on two basic principles: the user must grant each app authorisations for what it wants access to, and apps are strictly separated from one another. This way malware can only upload stolen data if it has been authorised for Internet access. However, proof-of-concept app Soundcomber bypasses all of this. It only requires authorisation for sound recording and disguises itself as a harmless voice memo app. It secretly taps phone calls and extracts numbers entered or spoken into the phone. It then transfers these numbers to its author by calling up the Android browser, which does not require authorisation. It directs the browser to go to a specific URL, which includes the numbers that have been stolen. The URL is interpreted by the author's server and he gains possession of the numbers. As an alternative, Soundcomber can also smuggle this data through a "dead postbox" to a second identical malware app. For this purpose, it changes the authorisations on different photos in your camera roll in a predetermined sequence. The information is then reassembled by the second app and then transferred via the Internet. Hackers can also transfer images this way.

Besides the camera and the microphone, a smartphone's motion sensors are also used to spy on users. This is supported by the research project (sp) iPhone, which uses the highly accurate accelerator sensors of an iPhone to determine what is

PHOTOS: NIKOLAUS SCHÄFFLER; INDIANA UNIVERSITY ILLUSTRATION: HARRY FUCHSLOCH

typed on a PC keyboard set beside the smartphone on the table. The smartphone registers the vibrations and reconstructs the text typed in from the sequence and a dictionary, although it helps if you know the subject matter that is being typed in advance. The researchers managed a success rate of 80 percent.

A walk through your apartment

Even scarier is what an app developed by the US Naval Surface Warfare Center does. Currently a research project, PlaceRaider can regularly take photos with your smartphone's cameras. It runs in the background and when taking photos, goes mute so there's no shutter sound. There is no way for the user to notice the unauthorised espionage. The app also analyses photos on the device, which can be done using the computing power of the smartphone. Badly lit and unclear photos as well as duplicates are removed. The app uploads the good photos to a remote server which is powerful enough to compose a panorama from multiple photos of the surroundings. Using several ordinary photos of a single area where the smartphone is located, a high-quality image can be extrapolated. With special software, the researchers can zoom into this panorama and even read text as tiny as the information on a cheque lying on a table, a scribble on a holiday calendar on the wall, or anything on your computer monitor. Criminals can even study the reconstructed 3D layout of your house or office in order to plan a break-in.

Protect yourself from smartphone spies

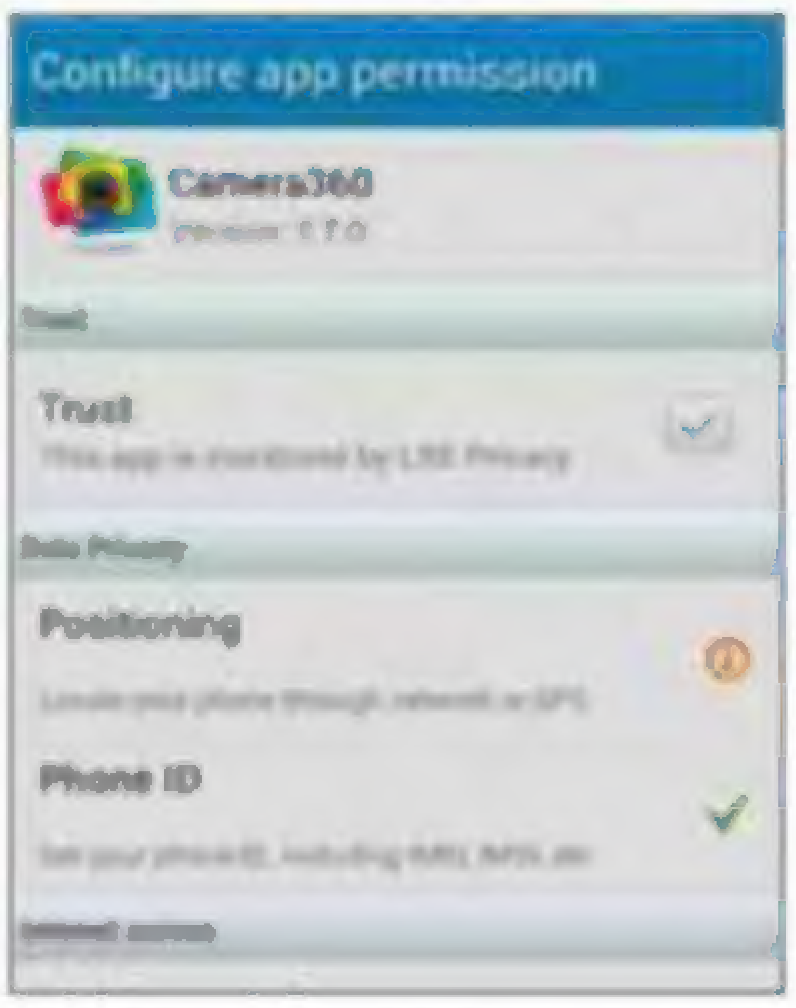
Even though the espionage apps mentioned here have only been used in research projects so far, it is only a matter of time until clever hackers start using them in real life—whether for good or for bad reasons. While iOS users enjoy a certain amount of protection due to Apple's store policies, users of Android devices must be really careful. Espionage is basically enabled by a combination of app authorisations (which users easily and often allow on Android mobile phones without much thought when installing an app). "Once an app receives authorisation to access the camera and the Internet, it can always take photos and videos and upload them," says Jan Böttcher, whose Hamburg-based company, Vukee.com, develops photo apps for Android and iOS. "That is why it is important to install apps only from reliable manufacturers and check the permissions they ask for."

In order to protect yourself from spies, you should allow camera and Internet access only to a few apps that have been developed by reliable sources. For increased protection, review your authorisations often. You can easily block a photo filters app from accessing the Internet. Processed photos are saved on your mobile phone, so you can publish them through the Android gallery instead. iOS users cannot control App Store applications as precisely but can depend on checks done by Apple prior to listing in the store.

In Apple's App Store for iOS, it is very difficult to find malicious apps, says Omar Abou Deif, head of app development at Vukee. Unlike Android, iOS apps can only remain active in the background if there is a very good reason for it doing so. Apple checks precisely why an app would like to run over a long period of time in the background and allows only a few to do so. No matter which platform you use, it is a good idea to uninstall apps that you don't use regularly—once an app is removed it no longer poses a threat.

MORE SECURITY: RESTRICT APPS

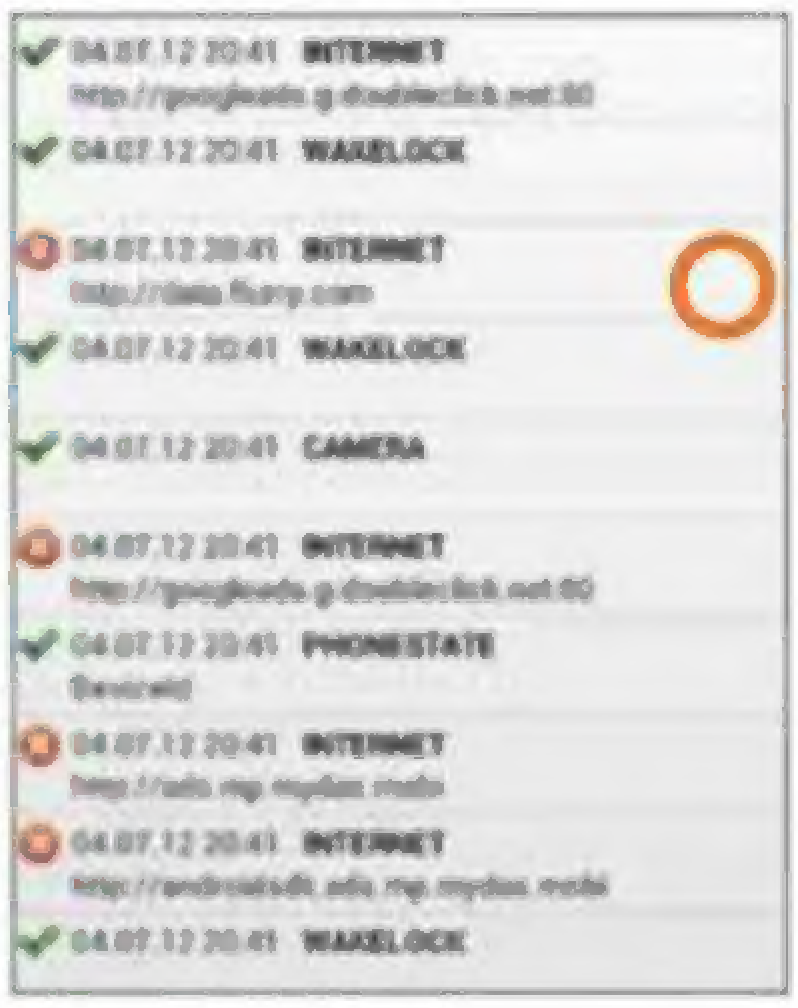
Don't just revisit your app permissions as an afterthought. Security apps such as LBE Privacy Guard (left) and SRT AppGuard (right) let you know what you're getting into and also revoke permissions which you may feel were granted by mistake.



Configure app permission

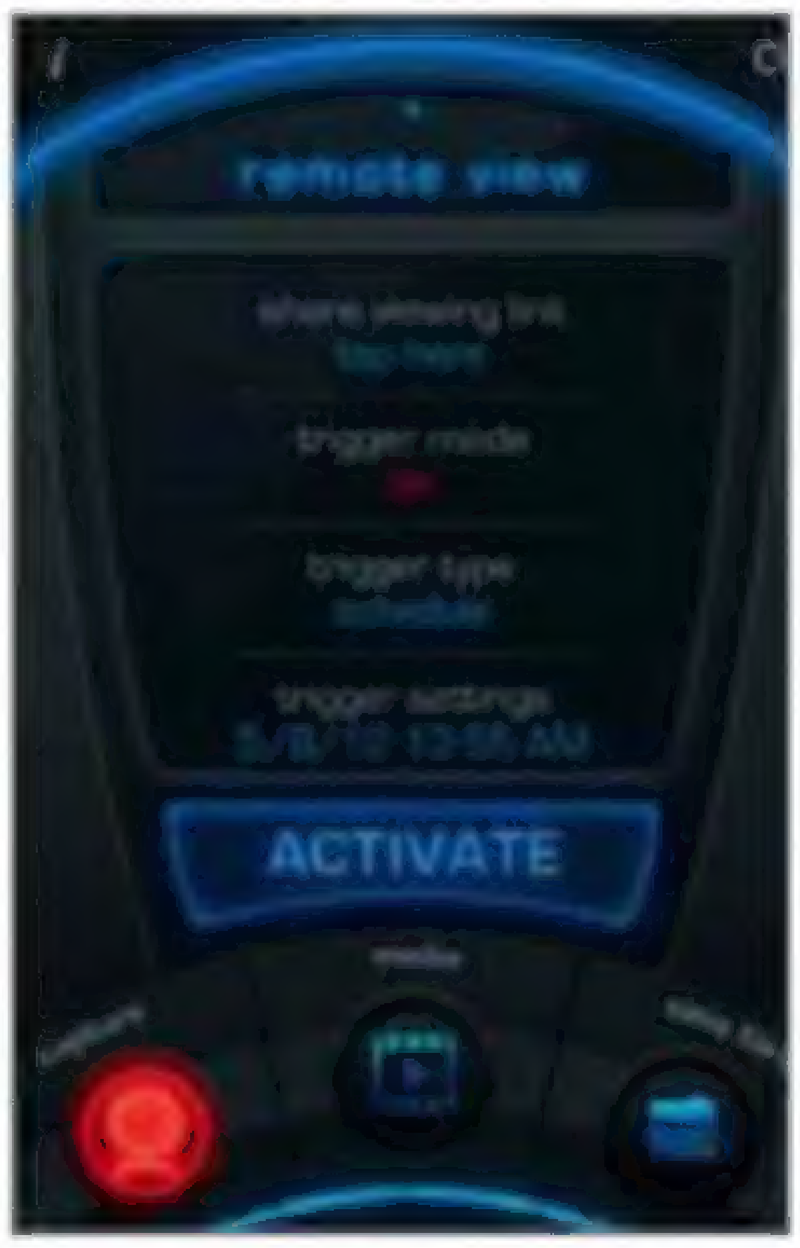
Camera360

LBE PRIVACY GUARD: Best suited to rooted Android devices. You can monitor internet traffic and block malicious apps.

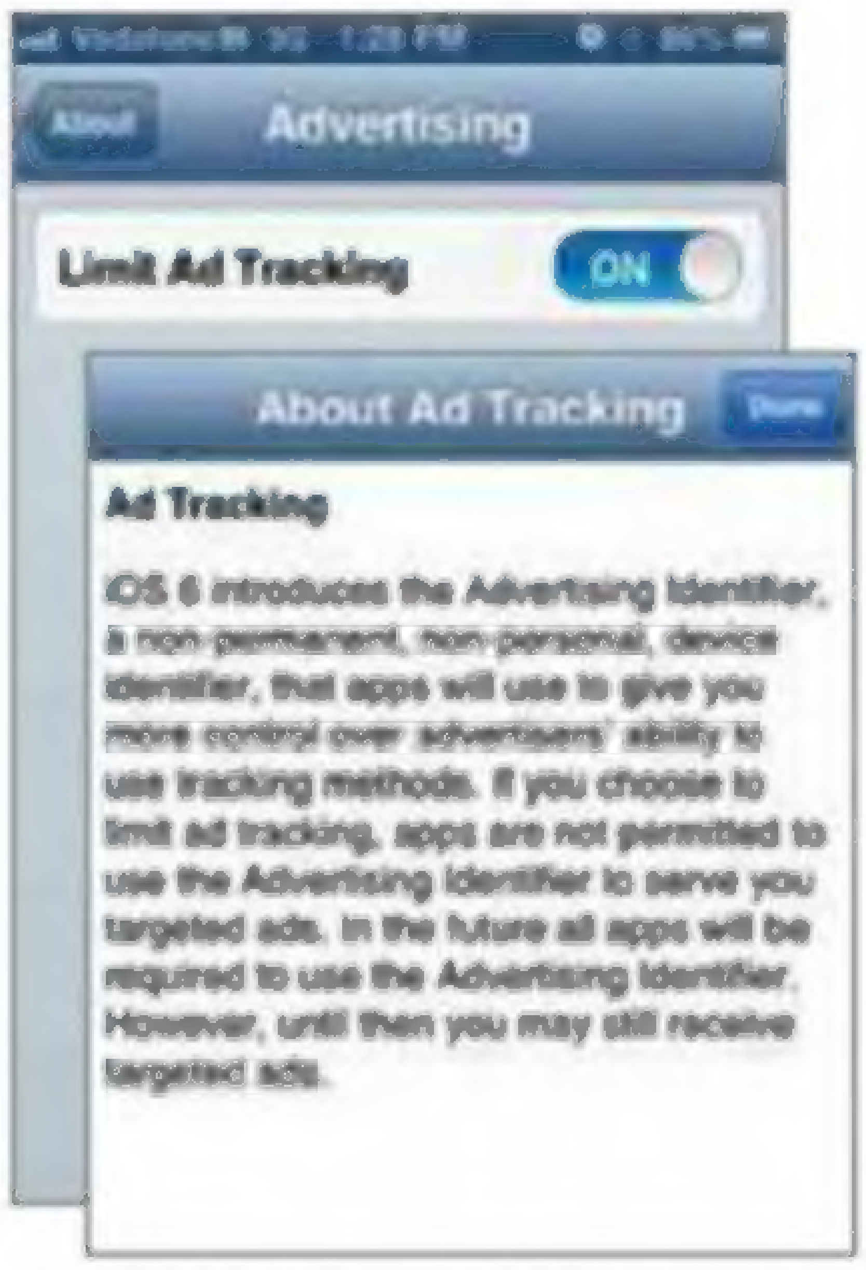


```
04.07.12 20:41 INTERNET
04.07.12 20:41 WAKELOCK
04.07.12 20:41 INTERNET
04.07.12 20:41 WAKELOCK
04.07.12 20:41 CAMERA
04.07.12 20:41 INTERNET
04.07.12 20:41 PHONESTATE
04.07.12 20:41 INTERNET
04.07.12 20:41 INTERNET
04.07.12 20:41 WAKELOCK
```

SRT APPGUARD: Not available in the Google Play store because it can alter other apps' permissions.



RECONBOT FOR iOS: Turns any iPhone into a secret webcam that keeps filming with a deceptive blank screen.



Limit Ad Tracking ON

About Ad Tracking

Ad Tracking

iOS 6 introduces the Advertising Identifier, a non-permanent, non-personal, device identifier, that apps will use to give you more control over advertisers' ability to use tracking methods. If you choose to limit ad tracking, apps are not permitted to use the Advertising Identifier to serve you targeted ads. In the future all apps will be required to use the Advertising Identifier. However, until then you may still receive targeted ads.

AD-TRACKING: The ad tracking settings of iOS can be found in 'Settings | General | About | Advertising'.

ON QUOTE

SEBASTIAN SCHREIBER, WHITE HAT HACKER AND PENETRATION TESTER

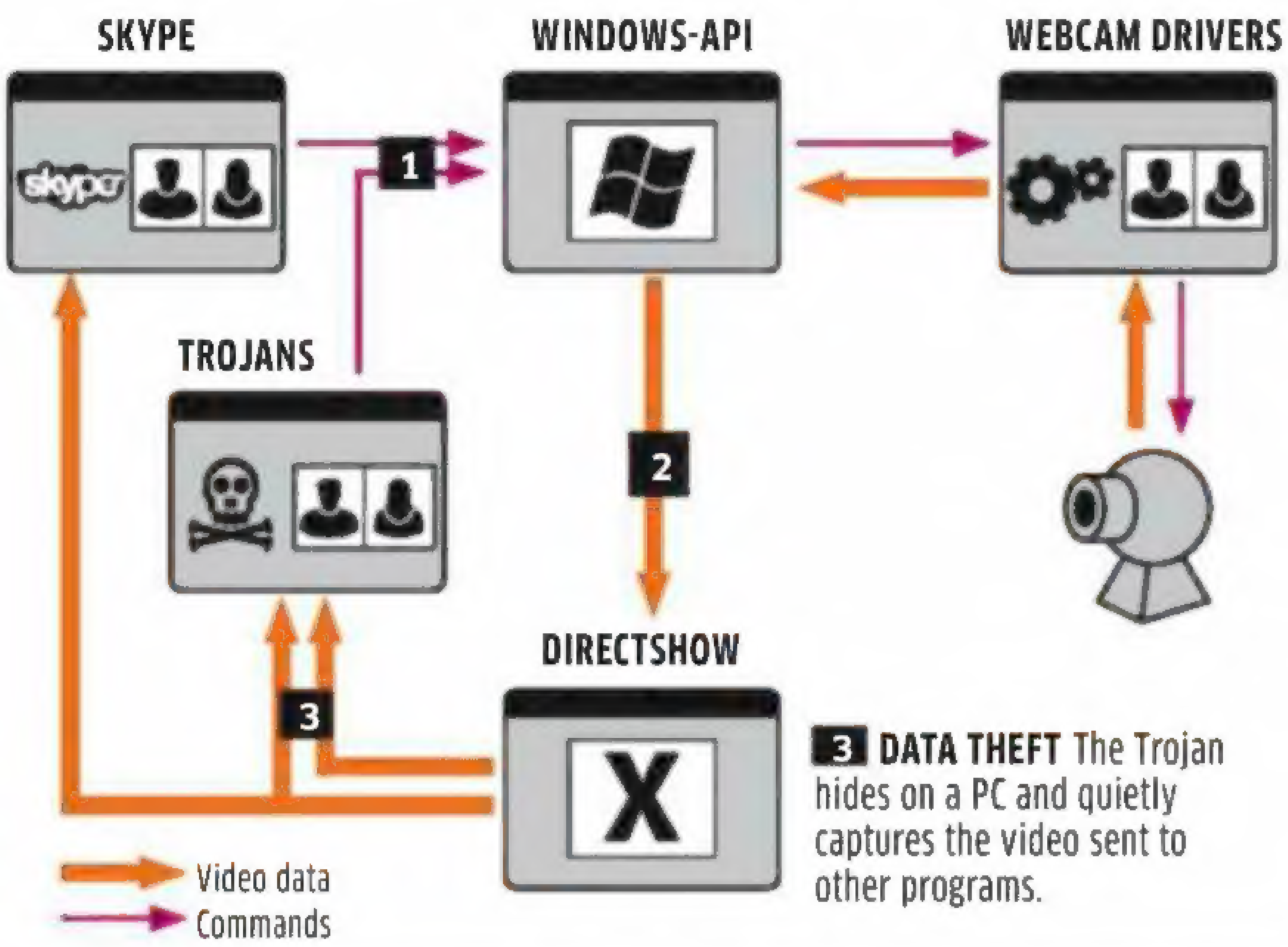
"From a financial perspective, spying via webcams is not profitable for criminal hackers. The low chance of success cannot justify the tremendous effort and time required to procure and analyse all the video and audio material that can be captured, as you can buy stolen credit card numbers today for quite a low price in certain circles. However, there are enough stalkers who target individuals to make this work. For video chat services such as Skype, the danger is not posed by criminals but by law enforcement authorities. The problem here is not local to the user, but rather at the service provider's level. In some cases they have to record and hand over data without the user's consent and without being able to object."

MALWARE TAPS INTO YOUR WEBCAM

A webcam trojan on your PC behaves exactly like legitimate software. Via standard API calls and DirectShow filters, the video stream can be diverted from a legitimate program and sent anywhere via the Internet, potentially unnoticed.

1 START RECORDING via an API call and the webcam driver won't know whether the source is malicious or not.

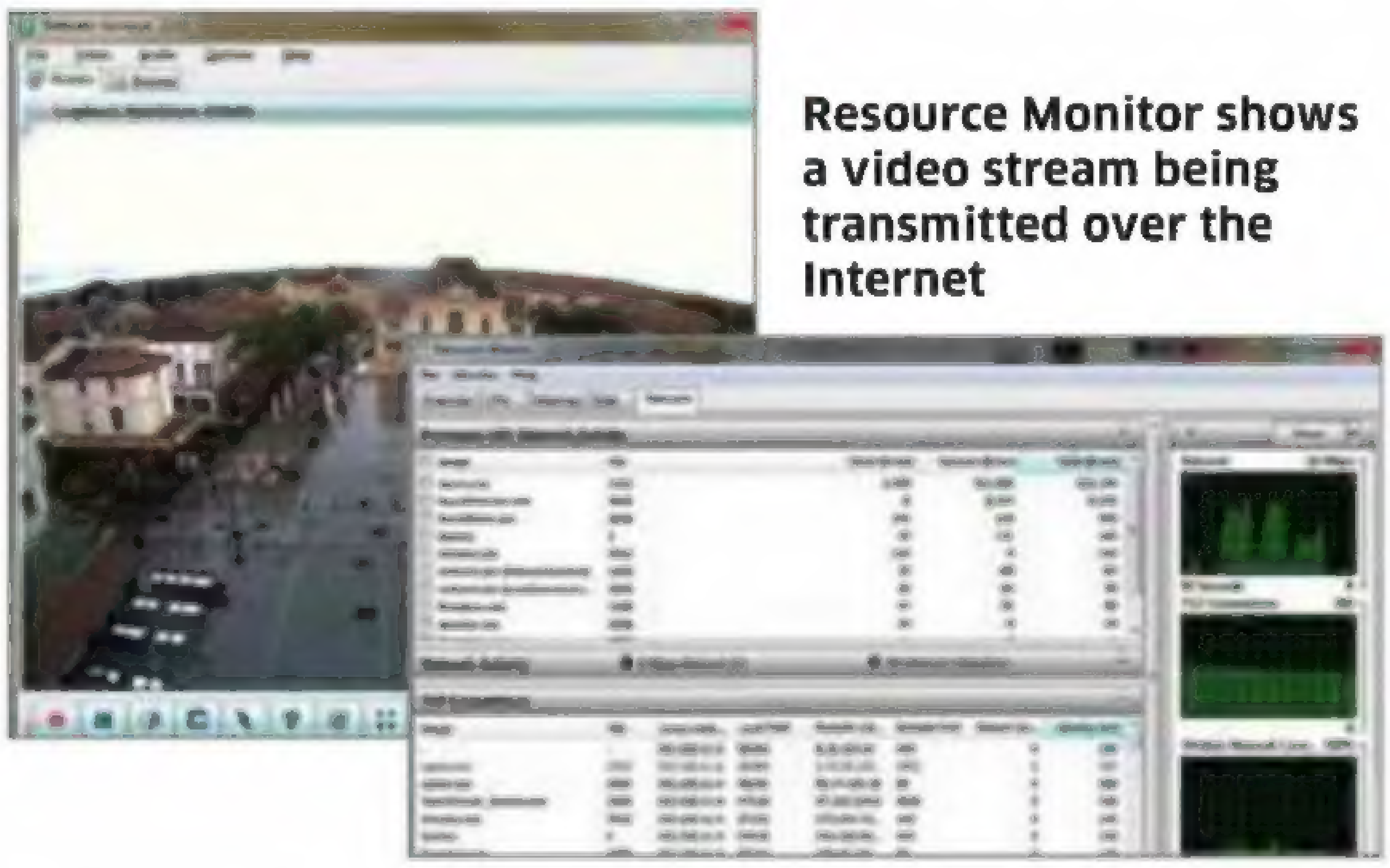
2 PROCESSING Windows APIs and DirectShow allow programs to access the webcam's stream.



3 DATA THEFT The Trojan hides on a PC and quietly captures the video sent to other programs.

HOW TO SPOT AN UNWANTED WEBCAM STREAM

A webcam surveyor can record or stream video without a user noticing anything. Type 'Resmon' in the Start menu search box to launch the Windows Resource Monitor, which will let you identify running processes as well as the network load each one produces.



Resource Monitor shows a video stream being transmitted over the Internet

MECHANICAL PROTECTION: SIMPLE, BUT EFFECTIVE

To be completely sure that you are not being spied on, unplug your webcam when it isn't in use or turn it to face a wall (though sound might still be recorded). For notebooks, this is not possible—so a simple piece of tape or a cover over the lens will do.

Special covers for the webcam lens look cleaner than adhesive stickers.

Simply turn the camera aside so that nothing of interest can be seen.

PC & NOTEBOOK

I can see you

Webcams have been around for quite a while, but now that they are so common, opportunities for misuse have increased.

Webcams have been available for PCs since the late 90s and are used mostly for video chats or simple supervision tasks. Many notebooks and all-in-one PCs have an integrated camera with a tiny lens placed on the top of the display. Any program installed on the computer can switch it on and photos or videos can be sent to any server on the Internet—ideally with the owner's knowledge and permission.

However, some American companies that offered computers on a hire-purchase basis took advantage of this option until the matter came to light in September 2012. Security software from DesignerWare was installed on PCs and notebooks to locate and block those computers for which installments had not been paid. Employees of seven rental agencies used this software illegally to access all kinds of information: private emails, and login credentials, including website and bank details. They also got hold of webcam photos of children and adults, who at times were naked or engaged in an intimate activity. The US Federal Trade Commission charged these companies with espionage and a settlement was reached. A similar case in 2010 involved schools in Pennsylvania spying on what students did at home through the webcams of Macbooks owned and administered by the schools, without anyone's knowledge. In yet another instance, a webcam espionage prank took a tragic turn with the suicide of an 18-year-old student, Tyler Clementi, of new Jersey. His roommate had filmed him secretly in compromising positions and tweeted about it, inviting others to view the live footage.

Simple ways to protect your privacy

An external USB webcam offers the most control: you can cover it when you are not using it, turn it aside, or simply unplug it from the USB port. The last option also disables the microphone, which many people forget to consider. Secure hardware covers are getting harder and harder to find for notebooks. Function keys that switch off the webcam don't offer 100 percent protection because the webcam can most likely be activated again with a software command. A solution would be to cover the webcam with black masking tape. If your webcam has an activity LED, pay careful attention: if it is often illuminated without a video chat or other relevant software running, even for just half a second at a time, you should immediately scan for malware.

As far as software goes, webcam espionage is usually carried out using backdoor Trojans, which is why the same measures generally recommended against malware are applicable: only install software from reliable sources, always update your antivirus, and use anti-spyware tools such as SpyBot Search & Destroy. Besides this, the Windows Firewall should always be active and you should only allow acceptable exceptions.

SMART TV

The TV's watching you this time

You can't really relax if you know somebody is watching you through the TV's webcam. Is this threat real?

The newest high-end TVs today come with integrated webcams. As with every product that has a camera and Internet connection, it is possible for the webcam to be secretly switched on and capture images. Smart TVs are quite an attractive target for malicious hackers and will be much more tempting if and when e-commerce activities via TV take off. To introduce malware into a smart TV, the attackers must develop an infected app that a user can voluntarily install. Another alternative is to install malware through websites the user surfs via the TV. This is difficult because of the several non-standard operating systems and browsers the manufacturers use. "Proprietary systems connected to the Internet through a home network router cannot be accessed from an external source", says Stefan Ortloff, virus analyst at Kaspersky Labs. However, ex-CIA chief David Petraeus was vocal about the agency's plans to use all options to tap smart TVs and other household devices of suspicious persons.

Block the spies in your living room

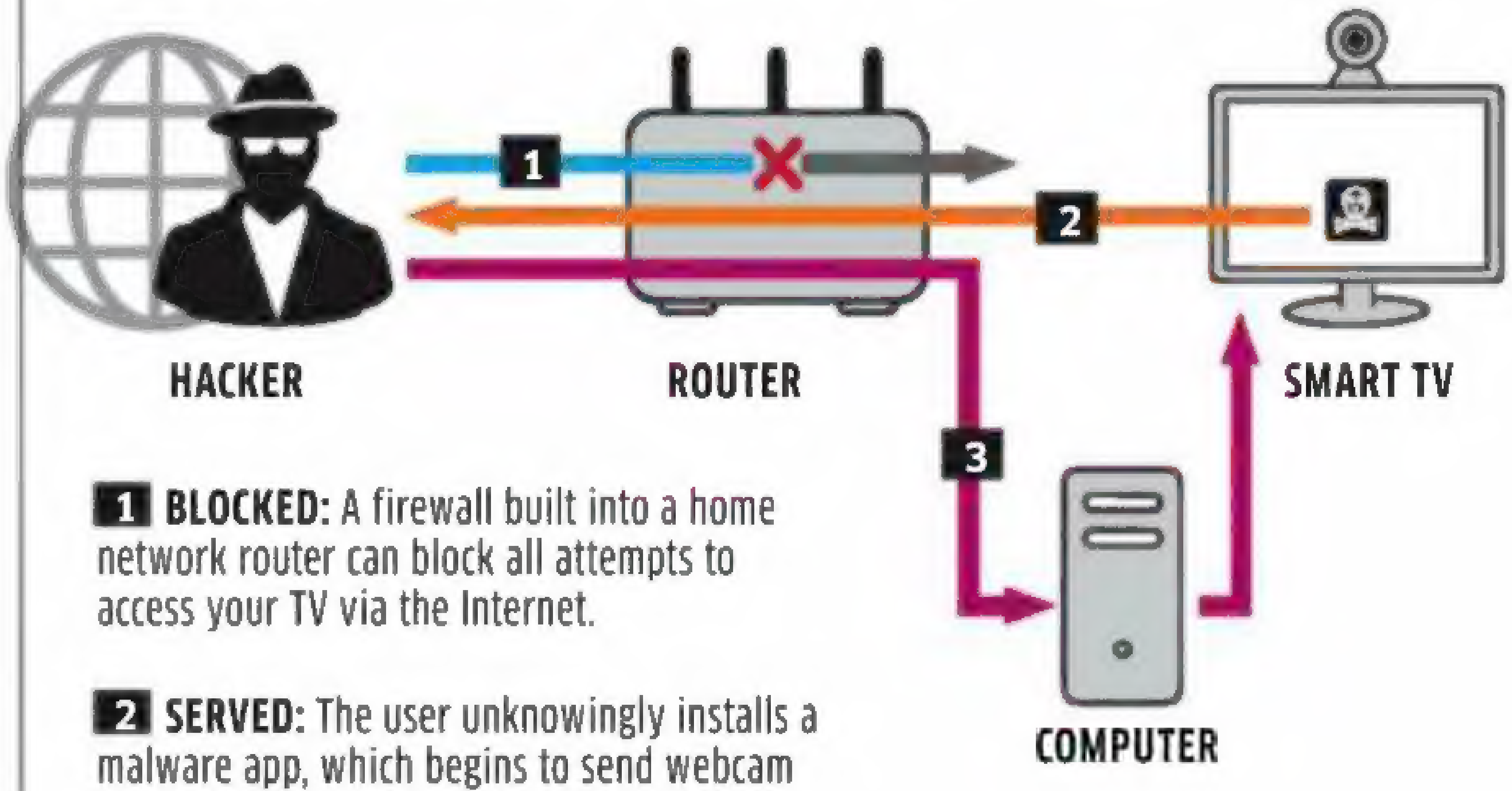
In order to check exactly which device communicates with which server, you will have to analyse your household data traffic. To do this, switch off all network devices except your PC and the device you wish to examine. Your router should let you see which devices are currently using the Internet connection and which IP addresses data is being sent to and received from. Get into the router's logs and monitoring capabilities by typing its IP address in your browser's address bar (usually 192.168.0.1). You will probably have to enter the admin password for the router. The exact way to access logs and monitor connections will vary for different router models and brands.

A tool that can be used to analyse packets, if you can capture them, is Wireshark. Routers flashed with the OpenWRT firmware can dump a text listing of packet traffic which Wireshark will analyse, or you can use tools such as AirCrack for Linux. Sort the packet list according to 'Source' in the tool, then scroll to the section in which the IP address of your television is listed as the source. Under 'Destination', you will see the servers with which the device has been communicating. www.whois.net will show you who operates the server and where it is located. If you find something suspicious, uninstall any app that might be generating suspicious traffic. To block any kind of communication with suspect servers, add their URLs or IP addresses to the router's blacklist through the settings page.

- feedback@chip.in

TELEVISION WEBCAMS: DIRECT AND INDIRECT ATTACKS

If a hacker wants to spy on your living room, malware can be sneaked onto your TV or a PC on the same home network. The TV's camera is switched on and transmits images. To stay safe, avoid installing apps from unknown sources.



1 BLOCKED: A firewall built into a home network router can block all attempts to access your TV via the Internet.

2 SERVED: The user unknowingly installs a malware app, which begins to send webcam images freely and unnoticed.

3 DETOUR: Malware on a PC in the home network can connect to the TV and infect it via the local home network.

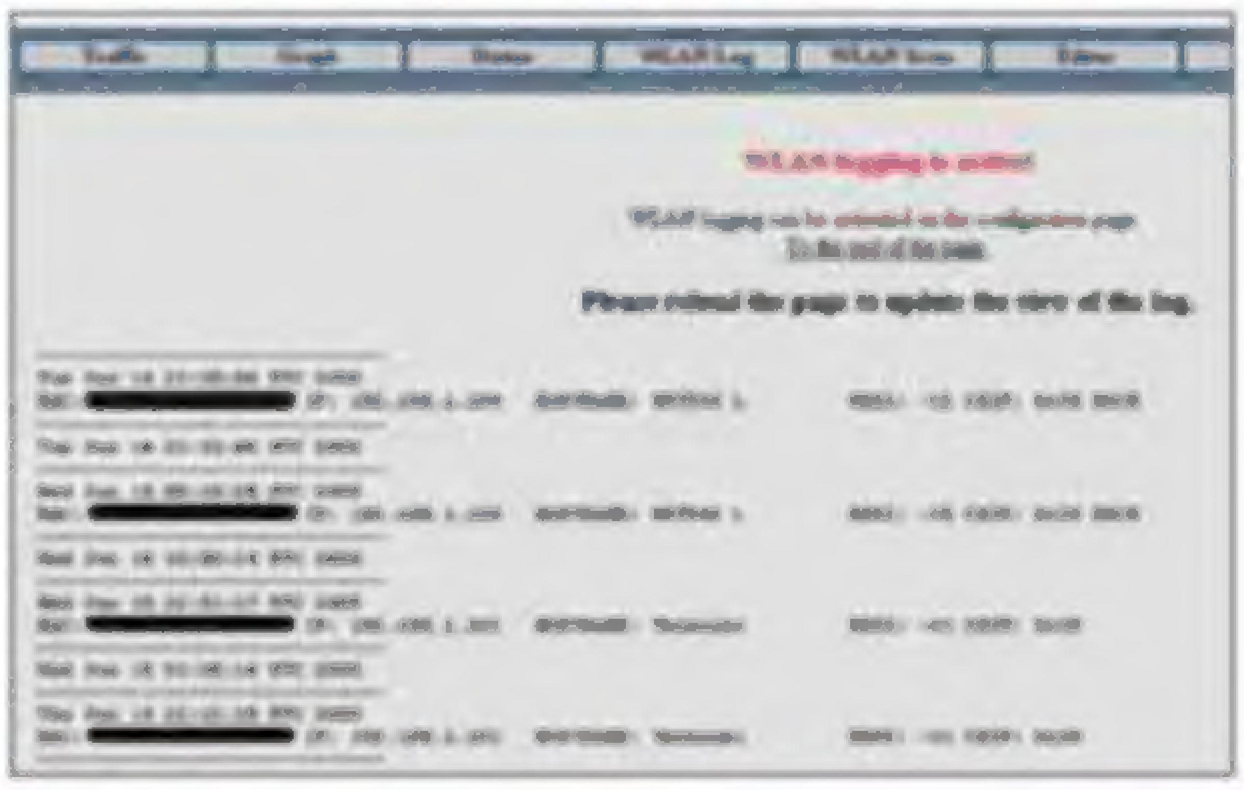
A PHYSICALLY SEPARATE CAMERA

Anyone who wants to feel completely safe from surveillance should, as with a PC webcam, simply unplug the camera when not in use, or if that is not possible, cover it with a physial barrier.

The webcams of Samsung Smart TVs can be turned until the lens disappears under a protective cover.

NETWORK TRAFFIC ANALYSIS AND RECORDING

While malware can hide its activity on the compromised device, it must transport the stolen data through your home router. Many models allow you to monitor traffic and other utilities will help you understand what is going on.



Go to the router's configuration page via your own web browser.

The tool Wireshark lets you analyse recorded data and identify where your data is being sent.